Perbandingan Proses Subtitusi S-Box DES dan S-Box AES Berdasarkan Nilai *Avalanche Effect* dan Nilai Kolerasi

Artikel Ilmiah

Peneliti:
Roby Jusepa (672008032)
Alz Danny Wowor, S.Si., M.Cs.

Program Studi Teknik Informatika
Fakultas Teknologi Informasi
Universitas Kristen SatyaWacana
Salatiga
April 2016

Perbandingan S-Box DES dan S-Box DES AES Berdasarkan Nilai Korelasi dan *Avalanche Effect* Terhadap Proses Subtitusi

Oleh,

Roby Jusepa
NIM : 672008032

Artikel Ilmiah

Diajukan Kepada Program Studi Teknik Informatika, Fakultas Teknologi Informasi
guna memenuhi sebagian dari persyaratan untuk mencapai gelar Sarjana Komputer

Disetujui oleh,

Alz Danny Wowor, S.Si., M.Cs.
Pembimbing

Diketahui oleh,

Dr. Dharmaputra T. Palekahelu, M.Pd.
Dekan

Suprihadi, S.Si., M.Kom.
Ketua Program Studi

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
SALATIGA
2016

Lembar Pengesahan

Judul Tugas Akhir	:	Perbandingan Proses Subtitusi S-Box DES dan S-Box AES Berdasarkan Nilai *Avalanche Effect* dan Nilai Kolerasi
Nama Mahasiswa	:	Roby Jusepa
NIM	:	672008032
Program Studi	:	Teknik Informatika
Fakultas	:	Teknologi Informasi

Menyetujui,

Alz Danny Wowor, S.Si., M.Cs.
Pembimbing

Mengesahkan,

Dr. Dharmaputra T. Palekahelu, M.Pd.	Suprihadi, S.Si., M.Kom.
Dekan	Ketua Program Studi

Dinyatakan Lulus Ujian tanggal : 4 Mei 2016

Penguji :

1. M.Ariance Ineke Pakereng, M.Kom.
2. Nina Setiyawati, S.Kom., M.Cs.

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN SATYA WACANA
Jalan Diponegoro 52 – 60
Phone. (0298) 321212 (Hunting)
Fax. (0298) 321433
E-mail: fti@uksw.edu
Salatiga 50711 – INDONESIA

LEMBAR PERSETUJUAN PUBLISH JURNAL

Dengan mempertimbangkan isi dari jurnal mahasiswa :

Nama Mahasiswa : Roby Juspa
NIM : 672008032

Maka jurnal ini dinyatakan :

~~LAYAK TERBIT~~ / TIDAK LAYAK TERBIT

Menyetujui,

(.....ALB.....)
Pembimbing 1

(.....)
Pembimbing 2

Mengetahui,

(M. A. Jusuf S.)
Penguji 1

(NINA SETYAWATI)
Penguji 2

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN TIDAK PLAGIAT

Saya yang bertanda tangan di bawah ini:

Nama : Roby Jusepa

NIM : 672008032 Email : Rbjusepa@yahoo.com

Fakultas : Teknologi Informasi Program Studi : Teknik Informatika

Judul tugas akhir : Perbandingan Proses Substitusi S-Box DES dan S-Box AES berdasarkan nilai Affalanche effect dan nilai kolerasi

Pembimbing : 1. Ir. Danny Wowor, S.Si., M.Cs

2. _____

Dengan ini menyatakan bahwa:

1. Hasil karya yang saya serahkan ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar kesarjanaan baik di Universitas Kristen Satya Wacana maupun di institusi pendidikan lainnya.
2. Hasil karya saya ini bukan saduran/terjemahan melainkan merupakan gagasan, rumusan, dan hasil pelaksanaan penelitian/implementasi saya sendiri, tanpa bantuan pihak lain, kecuali arahan pembimbing akademik dan narasumber penelitian.
3. Hasil karya saya ini merupakan hasil revisi terakhir setelah diujikan yang telah diketahui dan disetujui oleh pembimbing.
4. Dalam karya saya ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali yang digunakan sebagai acuan dalam naskah dengan menyebutkan nama pengarang dan dicantumkan dalam daftar pustaka.

Pernyataan ini saya buat dengan sesungguhnya. Apabila di kemudian hari terbukti ada penyimpangan dan ketidakbenaran dalam pernyataan ini maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya saya ini, serta sanksi lain yang sesuai dengan ketentuan yang berlaku di Universitas Kristen Satya Wacana.

Salatiga, 26 Mei 2016

Rp.6.000,-

Tanda tangan & nama terang mahasiswa

Roby Jusepa

F-LIB-080

PERPUSTAKAAN UNIVERSITAS
UNIVERSITAS KRISTEN SATYA WACANA
Jl. Diponegoro 52 – 60 Salatiga 50711
Jawa Tengah, Indonesia
Telp. 0298 – 321212, Fax. 0298 321433
Email: library@adm.uksw.edu ; http://library.uksw.edu

PERNYATAAN PERSETUJUAN AKSES

Saya yang bertanda tangan di bawah ini:

Nama : Roby jusepa
NIM : 672008032 Email : rbjusepa@yahoo.com
Fakultas : Teknologi Informasi Program Studi : Teknik Informatika
Judul tugas akhir : Perbandingan Proses Subtitusi S-Box DES dan S-Box AES berdasarkan nilai Aftalanche Effect dan nilai Koleasi

Dengan ini saya menyerahkan hak *non-eksklusif** kepada Perpustakaan Universitas – Universitas Kristen Satya Wacana untuk menyimpan, mengatur akses serta melakukan pengelolaan terhadap karya saya ini dengan mengacu pada ketentuan akses tugas akhir elektronik sebagai berikut (beri tanda pada kotak yang sesuai):

☑ a. Saya mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA

☐ b. Saya tidak mengijinkan karya tersebut diunggah ke dalam aplikasi Repositori Perpustakaan Universitas, dan/atau portal GARUDA**

* *Hak yang tidak terbatas hanya bagi satu pihak saja. Pengajar, peneliti, dan mahasiswa yang menyerahkan hak non-ekslusif kepada Repositori Perpustakaan Universitas saat mengumpulkan hasil karya mereka masih memiliki hak copyright atas karya tersebut.*

** *Hanya akan menampilkan halaman judul dan abstrak. Pilihan ini harus dilampiri dengan penjelasan/ alasan tertulis dari pembimbing TA dan diketahui oleh pimpinan fakultas (dekan/kaprodi).*

Demikian pernyataan ini saya buat dengan sebenarnya.

Salatiga, 26 Mei 2016

Roby jusepa
Tanda tangan & nama terang mahasiswa

Mengetahui,

Al. Danny Wowor, S.Si., M.Cs
Tanda tangan & nama terang pembimbing I

Tanda tangan & nama terang pembimbing II

F-LIB-081

Perbandingan S-box DES dan AES Berdasarkan Nilai Korelasi dan *Avalanche Effect* Terhadap Proses Subtitusi

[1] Roby Jusepa, [2]Alz Danny Wowor

Fakultas Teknologi Informasi
Universitas Kristen Satya Wacana
Jl. Diponegoro 52-60, Salatiga 50771, Indonesia
Email: [1]rbjusepa@yahoo.com, [2]alzdanny.wowor@staff.uksw.edu

Abstract

Within communicating an information, there is a method to secure data known as cryptography.In keeping our secret data, cryptography transforms plaintext to unrecognizable ciphertext. When it gets to the receiver, the ciphertext is transformed back to plaintext form so that it is recognizable. Many cryptography methods don't guarantee to be used forever, because the more cryptography techniques developed, the more cryptography experts who try to solve it. This observation observe the comparison of AES & DES, because according to logarithm, AEC logarithm replaces DES logarithm but not through S-box. Because in blockchiper principal, only sbox through logarithm that can make the relationship to be not linier. This observation adds comparison process of sbox DES & AES that would later be tested its correlation toward the Avalanche effect.

Keywords :*Comparison , sbox DES and AES , Avalanche effect.*

Abstrak

Dalam komunikasi suatu informasi terdapat sebuah metode pengamanan data yang dikenal dengan nama kriptografi.Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (*plaintext*) ke dalam bentuk data sandi (*ciphertext*) yang tidak dapat dikenali. Setelah sampai di penerima, *ciphertext* tersebut ditranformasikan kembali ke dalam bentuk *plaintext* agar dapat dikenali.Namun banyaknya teknik kriptografi tidak menjamin bisa untuk digunakan selamanya, karena semakin banyak teknik kriptografi dikembangkan makin banyak pula para ahli kriptanalisis mencoba untuk memecahkannya.Penelitian ini meneliti tentang perbandingan AES dan DES karena secara algoritma AES menggantikan algoritma DES tetapi tidak secara S-box. Karena dalam prinsip blokcipher hanya sbox yang secara algoritma mampu membuat hubungan yang tidak linier. Penelitian inimenambahkan proses perbandingan s-box DES dan AES berdasarkan Nilai Korelasi dan *Avalanche Effect* Terhadap Proses Subtitusi

Kata Kunci :Perbandingan, Sbox DES dan AES, *Avalanche effect*.

---

[1] Mahasiswa Fakultas Teknologi Informasi Program Studi Teknik Informatika, Universitas Kristen Satya Wacana Salatiga.
[2] Staff Pengajar Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana Salatiga

1. Pendahuluan

Kriptografi adalah ilmu yang mempelajari mengenai bagaimana cara mengamankan suatu informasi. Pengamanan ini dilakukan dengan mengenkripsi informasi tersebut dengan suatu kunci khusus. Informasi ini sebelum dienkripsi dinamakan plainteks. Setelah dienkripsi dengan suatu kunci dinamakan cipherteks. Keamanan suatu informasi agar tidak jatuh ke tangan orang-orang yang tidak berkepentingan sangatlah penting agar tidak disalahgunakan. Informasi ini dapat berupa *password*, nomor kartu kredit, ataupun informasi pribadi lainnya [1].

Kriptografi didefinisikan sebagai ilmu dan pelajaran untuk tulisan rahasia dengan pertimbangan bahwa komunikasi dan data dapat dikodekan untuk mencegah dari mata-mata atau orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu dan metode lainnya sehingga hanya orang yang berhak yang dapat mengetahui isi pesan sebenarnya. Dalam menjaga kerahasiaan data, kriptografi mentransformasikan data jelas (plainteks) ke dalam bentuk data sandi (cipherteks) yang tidak dapat dikenali. Cipherteks inilah yang kemudian dikirimkan oleh pengirim (*sender*) kepada penerima (*receiver*). Setelah sampai di penerima, cipherteks tersebut ditranformasikan kembali ke dalam bentuk plainteks agar dapat dikenali. Dalam arti lain, kriptografi adalah seni dan ilmu dalam mengamankan pesan.

S-box merupakan salah satu prinsip dalam perancangan blok cipher s-box salah satu prinsip blokcipher. Proses s-box itu sendiri mengganti karakter inputan dengan karakter yang sudah menjadi tetapan pada sebuah kotak. Secara teoritis,s-box adalah satu-satunya algoritma yang mempunyai kemampuanuntuk membuat hubungan yang tidak linier antara plainteks dan cipherteks.

Penelitianini membandingkan proses subtitusi dari dua kriptografi yang dijadikan standar pengamanan informasi oleh pemerintah Amerika Serikat yaitu S-box AES (*Advanced Encryption System*) dan DES(*Data Encryption System*).Pengujian dilakukan dengan melihat nilai korelasi dapat digunakan sebagai acuan untuk melihat proses subtitusi yang lebih unggul secara statistik.Pengujian yang lain adalah nilai *avalanche effect* digunakan untuk mengetahui perubahan sebuah inputbit pada plaintext dapat merubah berapa banyak bit yang berbeda di ciphertext.

2. Tinjauan Pustaka

Pada bagian ini akan membahas beberapa pustaka yang digunakan sebagai landasan teori yang dapat dijadikan acuan atau juga sebagai pembanding terkait perbandingan s-box DES dan AES.Berikut ini sebagai pustaka yang diacu adalah penelitian terdahulu yang telah dilakukan terkait dengan kriptografi DES dan kriptografi AES

Penelitian sebelumnya yang berjudul *Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques* menggunakan teknik *transposition* untuk meningkatkan keamanan kriptografi DES. Penelitian ini

menggunakan *plaintext* yang akan dienkripsi dengan algoritma DES yang sudah dimodifikasi dengan tambahan teknik *transposition*. Teknik *transposition* yang digunakan dalam penelitian ini adalah *Simple Columnar Transposition Technique* (SCTTMR). SCTTMR adalah teknik *transposition* yang menyusun *plaintext* ke dalam sebuah bujur sangkar atau tabel atau matriks dan membacanya dengan urutan kolom secara acak. Teknik SCTTMR dilakukan di awal proses enkripsi. Sehingga *plaintext* yang akan dienkripsi menggunakan algoritma DES sudah merupakan hasil dari modifikasi SCTTMR. Penelitian ini menghasilkan peningkatan keamanan pada algoritma DES. Jika *intruder* ingin menyerang algoritma modifikasi ini, maka diperlukan urutan *random* kolom yang digunakan pada proses SCTTMR dan memerlukan waktu yang lebih lama [3].

Penelitian lain yang berjudul *Modified Key Model of Data Encryption Standard* menggunakan 8 bit pertama hasil permutasi kompresi pertama dan 8 bit terakhir pada permutasi ke dua sebagai 16 bit kombinasi untuk tiap 48 bit *key* pada saat pengangkatan 16 kunci internal. Sehingga ketika dilakukan proses *enchipering* DES kunci yang digunakan 48 bit pada 16 bit pertama selalu statik atau sama. Tujuan dari penelitian ini adalah memperumit kriptografi DES normal pada saat pengangkatan kunci sehingga lebih sulit untuk dilakukan teknik kriptanalisis DES normal [4].

Hasil penelitian yang lain berjudul Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk Semua Jenis File. Hasil penelitian menunjukan bahwa algoritma AES dengan panjang kunci 256 bit dapat menyandikan isi suatu file sehinggadapat mengamankan file tersebut. Ukuran file enkripsi akan bertambah 11 *bytes* dari file asli karena adanya proses penambahan header yang berisi informasi ekstensi file [5].

Penelitian ketiga dengan topik "*Kombinasi Algoritma Rubik, CPSNRG Chaos dan S-Box Fungsi Linier dalam Perancangan Kriptografi Block Cipher*". Penelitian yang dilakukan Liwandouw & Wowor adalah menciptakan sebuah s-box dengan menggunakan fungsi linier yang dibangkitkan dari CPSNRG chaos berdasarkan inputan karakter kunci. Penelitian [6] dijadikan sebagai acuan untuk menguji variasi plainteks yang akan digunakan. Terdapat tiga bentuk plainteks yang digunakan diantaranya adalah plainteks biasa yang berupa karakter alfabet saja, kudua adalah karakter yang sama, dan ketiga karakter input yang merupakan kombinasi dari alfabet, simbol, angka, dan yang lainnya.

Berikut adalah definisi singkat mengenai DES dan AES. DES mengenkripsikan 64 bit plaintext menjadi 64 bit ciphertextdengan menggunakan 56 bit kunci internal (*internal key*) atauupa-kunci (*subkey*). Kunci internal dibangkitkan dari kuncieksternal (*external key*) yang panjangnya 64 bit [6].
Proses substitusi dilakukan dengan menggunakan delapan buah S-box yaitu S1 sampai S8. Setiap s-box menerima masukan 6 bit dan menghasilkan keluaran 4 bit. Kelompok 6-bit pertama menggunakan S1, kelompok 6-bit kedua menggunakan S2, dan seterusnya.

S-box yang berarti memetakan 6 bitS-box di dalam algoritma DES adalah 6 (4 baris×masukan menjadi 4 bit keluaran. Setiap S-box terdiri dari suatu tabel ukuran 4 dan 16 kolom). Setiap baris diberi nomor 0 sampai 3 dan setiap kolom diberi nomor 0 sampai 15. Masukan untuk proses substitusi adalah 6 bit

(b1b2b3b4b5b6). Nomor baris dari tabel ditunjukkan oleh string bit b1b6 (menyatakan nilai 0 sampai 3 desimal). Nomor kolom ditunjukkan oleh string bit b2b3b4b5 (menyatakan nilai 0 sampai 15 desimal).

S1

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

S2

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9

S3

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12

S4

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14

S5

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	16
2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3

S6

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13

S7

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12

S8

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Gambar 8. S-box DES [7]

Kriptografi *AES* adalah standar algoritma kriptografi terbaru yang menggantikan DES yang sudah dipecahkan. Algoritma ini termasuk kelompok kriptografi simetris yang berbasis pada blok cipher.

Sebuah tabel s-box terdiri dari 16×16 baris dan kolom dengan masing-masing berukuran 1 *byte*. Tabel s-box diperlihatkan pada Gambar 9.

		Y															
	HEX	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
	0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
	1	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
	2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
	3	04	c7	23	c3	18	96	05	9a	7	12	80	e2	eb	27	b2	75
	4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
	5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
	6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
X	7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
	8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
	9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
	a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
	b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
	c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
	d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
	e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
	f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Gambar 9. S-Box AES [10]

Pengujian algoritma kriptografi dilakukan dengan menggunakan korelasi. Teknik Statistik yang dipergunakan untuk mengukur kekuatan hubungan 2 variabel dan juga untuk dapat mengetahui bentuk hubungan antara 2 variabel tersebut dengan hasil yang sifatnya kuantitatif. Kekuatan hubungan antara 2 variabel yang dimaksud adalah apakah hubungan tersebut erat, lemah, ataupun tidak erat sedangkan bentuk hubungannya adalah apakah bentuk korelasinya *linier* positif ataupun *linier* negatif. Kekuatan hubungan antara 2 variabel biasanya

disebut dengan koefisien korelasi dan dilambangkan dengan *symbol* "*r*". Nilai koefisian *r* akan selalu berada di antara -1 sampai +1.

Koefisien korelasi sederhana disebut juga dengan koefisien korelasi *pearson*. Dimana "*r*" didapat dari jumlah nilai selisih perkalian antara *x* dan *y* dengan hasil perkalian jumlah total *x* dan *y* dibagi dengan hasil akar dari selisih perkalian jumlah *x* kuadrat dengan kuadrat pangkat dua untuk jumlah total *x* dengan selisih jumlah *y* kuadrat dengan kuadrat pangkat dua untuk total *y* dimana *x* sebagai plainteks dan *y* sebagai cipherteks. Maka Persamaannya adalah [5]:

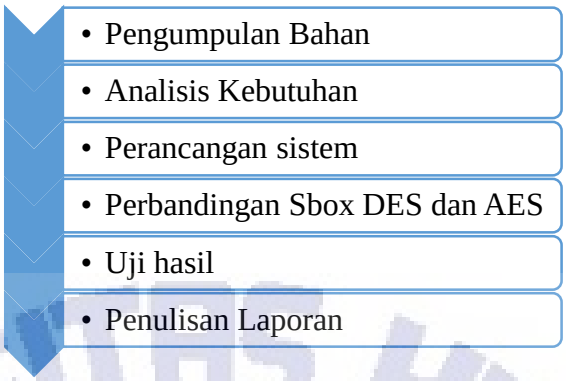
$$r = \frac{n\sum xy - \sum x \sum y}{\sqrt{\{n\sum x^2 - (\sum x)^2\}\{n\sum y^2 - (\sum y)^2\}}} \quad (1)$$

Salah satu pengujian yang sering digunakan untuk menentukan baik atau tidaknya suatu algoritma kriptografi blokcipher adalah dengan melihat nilai *avalanche effect* (AE). Perubahan yang kecil pada *plainteks*atau inputan dengan kunci tetap, dan melihat perubahan yang terjadi pada*cipherteks*. Semakin tinggi nilai AE akan semakin baik, menujukkan kekuatan algortima yang dapat membuat input tidak bisa dengan mudah secara langsung dilihat hubungannya dengan output. Kegunaan lain dari pencarian nilai AE adalah membuat perbedaan yang cukup sulit untuk kriptanalis melakukan serangan [4]. Bentuk umum untuk menentukan nilai *AE* dirumuskan pada Persamaan (2).

$$Avalanche\,Effect\,(AE) = \frac{\sum bit\ berbeda}{\sum bit\ total} \times 100\% \quad (2)$$

3. Metode Penelitian

Penelitian ini dilakukan melalui tahapan penelitian yang terbagi dalam dalam enam tahapan, yaitu: (1) Pengumpulan bahan, (2) Analisis kebutuhan, (3) Perancangan sistem, (4) Perbandingan Sbox DES dan AES, (5) Uji hasil, dan (6) Penulisan laporan.



Gambar 10. Langkah-langkah Penelitian

Langkah 1:Pengumpulan bahan yaitu, melakukan pengumpulan terhadap data-data dari jurnal-jurnal, buku, serta sumber yang terkait dengan pada DES dan AES; Langkah 2: Analisis kebutuhan yaitu, melakukan analisis mengenai kebutuhan apa saja yang dibutuhkan dalam perancangan Sbox DES dan AES;Langkah 3: Perancangan sistem, yaitu langkah dimana membuat bagan proses enkripsi serta gambaran-gambaran umum mengenai perbandingan yang akan dilakukan; Langkah4: Membandingkan S-box DES dan AES yaitu, melakukan perbandingan berdasarkan tahap ketiga kemudian melakukan analisis hasil dari S-box DES dan AES untuk mendapatkan hasil akhir dari kedua sbox tersebut; Langkah 5: Uji Hasil yaitu, melakukan uji hasil terhadap keseluruhan perancangan dan perbandingan yang telah dibuat; Langkah 6: Penulisan laporan hasil penelitian yaitu, mendokumentasikan proses penelitian yang sudah dilakukan dari tahap awal hingga akhir kedalam tulisan, yang akan menjadi laporan hasil penelitian.

4. Hasil dan Pembahasan

Implementasi algoritma kriptografi DES pada ukuran blok 64 bit. DES mengenkripsikan 64 bit plaintext menjadi 64 bit ciphertext dengan menggunakan 56 kunci internal (*internal key*) atau upa-kunci (*subkey*). Kunci internal dibangkitkan dari kunci eksternal (*external key*) yang panjangnya 64 bit.

Langkah–langkah untuk mengenkripsi data menggunakan algoritma DES dilakukan dengan mengkonversi setiap karakter ke dalam ASCII dan kemudian ke dalam bit. Konversi bit perlu dilakukan untuk dapat menyesuaikan kedalam s-box DES yang hanya menerima input 6 bit. Tabel 1 menunjukkan proses perubahan dari masukan menjadi bit berdasarkan karakter ASCII.Sebagai Plaintext “FTI UKSW”dengan 64bit.

Tabel 1. Proses Konversi Inputan ke ASCII dan Bit

F	T	I		U	K	S	W
70	84	73	32	85	75	83	87
01000110	01010100	01001001	00100000	01010101	01001011	01010011	01010111
0100011001010100010010100010000001010101010010110101001101010111							

Pada tabel 1 dijelaskan plainteks “FTI UKSW” dimana setiap biner dari plainteks tersebut akan digabung dari setiap plainteks setelah itu dari setiap biner tersebut akan di bagi lagi menjadi 6 bit untuk dapat diproses lagi kedalam s-box maka akan didapatkan hasil seperti padaTabel 2.

Tabel2. Perpotongan Bit

1	7	13	19	25	31	37	43
010001	100101	010001	001001	001000	000101	010101	001011

Langkah selanjutnya dari hasil padaTabel 2 setiap biner akan diekspansi untuk dilanjutkan proses inputan kedalam s-box dengan langkah awal pada plainteks “FTI UKSW” maka dilakukan pengambilan bitouter dibagian awal dan akhir 6 bit dari setiap karakter untuk dapat diproses lagi kedalam S-box,ditunjukkan pada Tabel 3.

Tabel 3. Ekspansi.

F	T	I		U	K	S	W
0	1	0	0	0	0	0	0
1000	0010	1000	0100	0100	0010	1010	0101
1	1	1	1	0	1	1	1

Setelah mendapatkan hasil ekspansi dari proses sebelumnya maka proses selanjutnya akan disubtitusikan kedalam tabel S-box, dimana blok pertama disubtitusikan dengan tabel S1. Kemudian kita ambil sampel blok bit pertama dari “F” yaitu **0**10001**1**. Dipisahkan blok menjadi 2 bit pertama dan terakhir yaitu “0” dan “1” digabungkan menjadi “01” disebut juga (outer) dan Bit kedua hingga ke lima 1000 ditunjukan pada tabel 3 Kemudian dibandingkan dengan memeriksa perpotongan antara keduanya didapatkan nilai 1010 (warna biru) dengan hasil akhir dari s-box. Seperti pada tabel 4.

Tabel 4. Pencocokan S-Box.

outer	binner	untuk pencocokan	hasil dari sbox	biner
01	1000	011000	10	1010
11	0010	110010	10	1010
01	1000	011000	2	0010
01	0100	010100	6	0110
00	0100	000100	7	0111
01	0010	010010	4	0100
01	1010	011010	5	0101
01	0101	010101	3	0011

Pengujian nilai *Avalanche effect*pada s-box DES dengan membandingkan nilai bit yang berbeda pada ciphetext dengan membandingkan dua palintext yang hanya berbeda 1 bit. Pengujian dilakukan dengan memilih inputan pertama adalah “FTI UKSW” dan yang kedua “FTJ UKSW”.

FTI UKSW							
1010	1010	0010	0110	0111	0100	0101	0011
1	1	0	0	0	0	0	0
0	0	0	1	1	1	1	0
1	1	1	1	1	0	0	1
0	0	0	0	1	0	1	1

Gambar 11. Output Bit "FTI UKSW"

FTJ UKSW							
1010	1010	0010	0110	0111	0100	0101	0011
1	1	0	0	0	0	0	0
0	0	0	1	1	1	1	0
1	1	1	1	1	0	0	1
0	0	0	0	1	0	1	1

Gambar 12. Output Bit "FTJ UKSW"

Pengujian pada s-box DES dengan inputan "FTI UKSW" ditunjukkan pada Gambar 11, sedangkan untuk plaintext "FTJ UKSW" diberikan pada Gambar 12. Persamaan (2) digunakan untuk melihat seberapa banyak nilai AE bila masukan hanya berbeda 1 karakter.ditunjukan padaTabel 5.

Tabel 5. Nilai *Avalanche effect*

HASIL							
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

Berdasarkan hasil perhitungan antara kedua plaintext padaTabel 5 didapatkan hasil sebagai berikut dengan hasil bit dan nilai *avalanche* nya ada "0". Berikutnya perhitungan nilai *Avalanche effect* pada s-box AES dengan cara dan proses yang sama pada s-box DES dengan membandingkan dua palintext yang hanya berbeda 1 bit. Pengujian dilakukan dengan memilih inputan pertama adalah "FTI UKSW"pada table 6 dan yang kedua "FTJ UKSW" pada Tabel 7.

Tabel 6.Output Bit "FTI UKSW"

01011010	00100000	00111011	10110111	11111100	10110011	11101101	01011011
0	0	0	1	1	1	1	0
1	0	0	0	1	0	1	1
0	1	1	1	1	1	1	0
1	0	1	1	1	1	0	1
1	0	1	0	1	0	1	1
0	0	0	1	1	0	1	0
1	0	1	1	0	1	0	1
0	0	1	1	0	1	1	1

Tabel 7.Output Bit "FTJ UKSW"

01011010	00100000	11010110	10110111	11111100	10110011	11101101	01011011

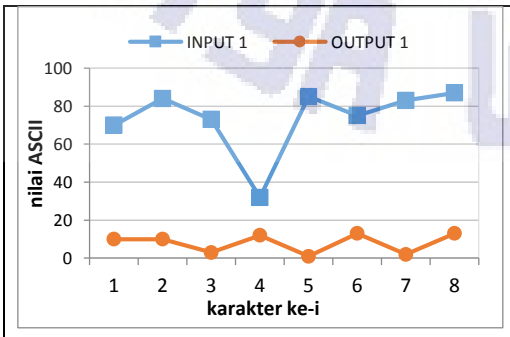
0	0	1	1	1	1	1	0
1	0	1	0	1	0	1	1
0	1	0	1	1	1	1	0
1	0	1	1	1	1	0	1
1	0	0	0	1	0	1	1
0	0	1	1	1	0	1	0
1	0	1	1	0	1	0	1
0	0	0	1	0	1	1	1

Hasil perhitungan antara kedua plaintext tersebut dengan merubah 1 bit yang berbeda maka didapatkan hasil sebagai berikut dengan hasil nilai *avalanche* nya adalah "9.375"

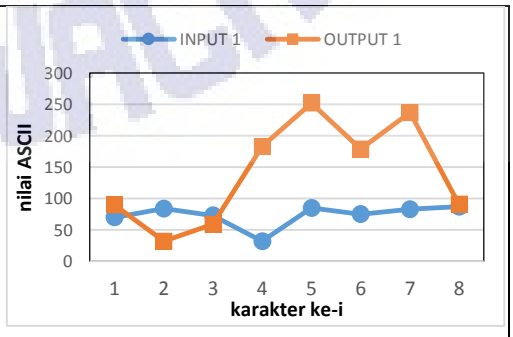
Tabel8.Nilai *Avalanche effect*

HASIL							
0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	1	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	1	0	0	0	0	0

Untuk Algoritma AES. Sebuah tabel S-Box terdiri dari 16x16 baris dan kolom dengan masing-masing berukuran 1 *byte*. Tabel S-Box diperlihatkan pada Gambar 8.



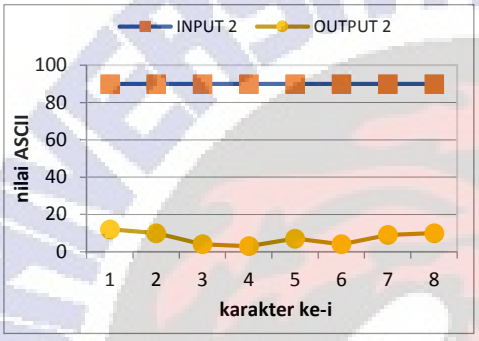
Gambar 13. Input dan Output "FTI UKSW" pada DES



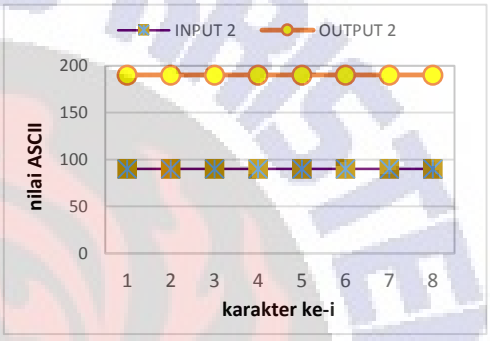
Gambar 14. Input dan Output "FTI UKSW" pada AES

Proses berikutnya akan dilakukan untuk s-box DES dari plainteks “FTI UKSW” tersebut dengan masukan “70, 84, 73, 32, 85, 75, 83, 87” dengan menghasilkan output “ 10, 10, 2, 6, 7, 4, 5, 3” dan melakukan uji statistic berdasarkan input dan output dari “FTI UKSW” yang menghasilkan nilai kolerasi s-box DES berikut: -0.030230148. gambar 13.

Selanjutnya dilakukan proses perhitungan kolerasi pada s-box AES dengan inputan nilaiinput dan output dari plainteks “FTI UKSW” dengan ambilan nilai ASCII “70, 74, 73, 32, 85, 75, 83, 87” dan nilai decimal “90, 32, 59, 183, 252, 179, 237, 91” dengan hasil kolerasi -0.105014104 dapat dilihat pada gambar 14.



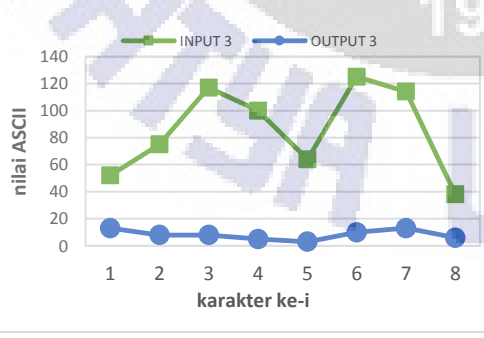
Gambar 15. Input dan Output “ZZZZZZZZ” pada DES



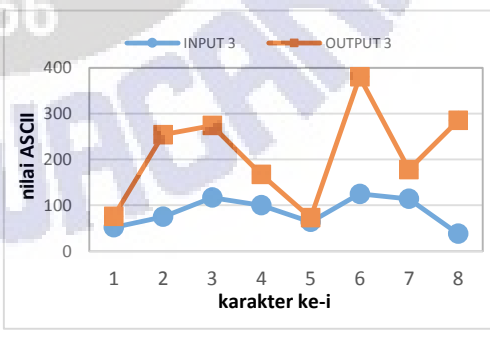
Gambar 16. Input dan Output “ZZZZZZZZ” pada AES

Berikutnya hasil uji nilai “Z” pada s-box DES adalah “90, 90, 90, 90, 90, 90, 90, 90” dengan hasil s-box “ 12, 10, 6, 12, 15, 2, 1, 0 ” dengan nilai kolerasi tidak terdefinisi pada gambar 15.

Berikutnya hasil pengujian nilai “Z” pada s-box DES adalah “90, 90, 90, 90, 90, 90, 90, 90” dengan hasil s-box “ 190, 190, 190, 190, 190, 190, 190, 190 ” dengan nilai kolerasi tidak terdefinisi dapat dilihat pada gambar 16.



Gambar 17. Input dan Output “4Kud@}r&” pada DES



Gambar 18. Input dan Output “4Kud@}r&” pada AES

Untuk gambar 17 dijelaskan bahwa hasil pengujian plaintext “4Kud@}r&” pada s-box DES adalah “52, 75, 117, 100, 64, 125, 114, 38” dengan hasil s-box “ 13, 8, 8, 5, 3, 10, 13, 6” dengan nilai kolerasi 0.256377862.

Berikutnya hasil pengujian plaintext “4Kud@}r&” pada s-box AES adalah “52, 75, 117, 100, 64, 125, 114, 38” dengan hasil s-box “24, 179, 157, 67, 9, 255, 64, 247” dengan hasil kolerasi 0.137656837 pada gambar 18. Dengan hasil nilai korelasi dari perbandingan antara s-box Des dan s-box AES yang memiliki nilai korelasi terendah adalah DES -0.030230148, menunjukkan bahwa s-box DES cukup baik dalam mengacak bit plaintext.

5. Kesimpulan

Penelitian ini meneliti tentang perbandingan AES dan DES karena secara algoritma, algoritma AES menggantikan algoritma DES tetapi tidak secara s-box. Karena dalam prinsip blokcipher hanya s-box yang secara algoritma mampu membuat hubungan yang tidak linier. Kriptografi s-box Des akan lebih efektif apabila jumlah bit plaintextnya dalam jumlah besar. Berdasarkan perbandingan efesiensi bit ciphertext antara dua rancangan kriptografi s-box AES dan DES, dapat disimpulkan sebelum dilakukan proses kedalam s-box maka dilakukan proses ekspansi untuk mendapatkan hasil ciphertext yang lebih efesiensi. Selain itu penelitian ini juga dapat digunakan sebagai metodologi baru dalam kriptografi simetris yang dapat membantu penelitian kriptografi.

6. Daftar Pustaka

[1] Didi Surian, 2006. Algoritma Kriptografi AES RIJNDAEL.

[2] Suprabowo, Arif. 2011. *Analisa Kriptanalisis Deferensial Pada Twofish*. Institut Teknologi Bandung.

[3] Sunil, S., Maakar, K., & Kumar, S., 2015,*Enhancing the Security of DES Algorithm Using Transposition Cryptography Techniques, International Journal of Advanced Research in Computer Science and Software Engineering*, http://www.ijarcsse.com/docs/papers/Volume_3/6_June2015/V3I6-0267.pdf (diakses tanggal 17 Febuari 2016).

[4] Salih, M.,2010,*ModifiedKey Model of Data Encryption Standard*,College of Engineering, University of Anbar, Iraq. http://www.iasj.net/iasj?func=fulltext&aID=14266.pdf (diakses tanggal 12 maret 2016)

[5] Yuniati, V., Indrianta, G.,&Rachmat, A., 2009,*Enkripsi dan Dekripsi dengan Algoritma AES 256 untuk semua jenis file*:Yogyakarta. http://ti.ukdw.ac.id/ojs/index.php/informatika/article/viewfile/69/29 (diakses tanggal 12 maret 2016)

[6] Liwandow, V. B., & Wowor, A. D., 2015, Kombinasi Algoritma Rubik, CPSNRG Chaos dan S-Box Fungsi Linier dalam Perancangan Kriptografi Block Cipher, *Seminar Nasional Sistem Informasi Indonesia* (SESINDO), Surabaya: Program Studi Sistem Informasi, ITS.

[7] Munir, Rinaldi. 2006. Kriptografi. Bandung: Penerbit Informatika.

[8] Rijndael S-box, URL: http://en.wikipedia.org/wiki/Rijndael_S-box (diakses pada tanggal 15 maret 2016).
[10] Sbox DES
[11] Vazhayil, A, 2015, *Advanced Encryption Standard: S-Box*, Di unduh: https://captanu.wordpress.com/tag/aes/ (16 Maret 2016)